REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

This amendment adds, changes and/or deletes claims in this application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

After amending the claims as set forth above, claims 1-91 are now pending in this application.

Claims 1, 4-6, 36, 52, 58, 60, 61, 63, 64, 65, 66, 68, 70, 71, 73, 74, 75, 76, 78, and 80 have been amended.

Selected claims have been rejected under 35 USC – 103 (a) over Kanda et al. (6,769,063) in view of Zeidler (4,423,287), or under 35 USC – 103 (a) over Kanda et al. (6,769,063) in view of Zeidler (4,423,287) and further view of Jones et al. (6,434,699), or under 35 USC – 103 (a) over Kanda et al. (6,769,063) in view of Zeidler (4,423,287) and further view of Bellare et al. (5,757,913). These rejections are respectfully traversed and reconsideration thereof is requested.

The references to Kanda et al. in view of Zeidler are deficient and do not meet the claim language for at least the following reasons:

All of the rejections are premised on the base reference of Kanda modified by teachings in Ziedler. However, this combination of references is missing basic elements in the claims. Referring to claim 1, the step is provided of "after said applying step, combining said plurality of enciphered blocks to create an authentication tag," in the claimed combination of "partitioning said data into a plurality of data blocks;" "for each of said data blocks, performing a randomization function over said data block to create an input block of the same size as that of said data block, said input block not including a block identifier;"

"applying a pseudo-random function to each said input block to create a plurality of enciphered blocks." The sequence is evident from the claim language. Namely, data blocks are obtained by partitioning. This is followed by performing a randomization function to obtain input blocks. This step is followed by applying a pseudo-random function to each said input block to create a plurality of enciphered blocks. Thus, a sequence is set up. The resulting "enciphered blocks" are then combined to create an authentication tag. The "combining step could not occur until the encipher blocks have been created.

Although this sequence is clear from the claim language, an amendment "after said applying step" has been made to further clarify the point.

Referring to Kanda, the office action at page 3 notes that "Kanda does not disclose combining the plurality of enciphered blocks to create an authentication tag." This deficiency in Kanda is stated to be made up by Zeidler. However, Zeidler does not create an authentication tag by a combining step. Rather, in FIG. 3 (element 62, described at column 11, lines 5-15), Zeidler simply inputs an encrypted PIN into the standard, sequential CBC-MAC computation that is described in FIG. 13. In FIG. 13 and col. 16, lines 1-2, Zeidler describes applying a first block of data along with a key to a DES cycle block 164 and then exclusive-oring the result with the next block of data and applying the result to a second DES block 172, in a sequence. The end result of multiple exclusive-oring of the previous result with the next block of data in sequence is the output of the cycle block 182, i.e., a 64 bit ciphertext, which is then truncated to obtain block 186, the 24-bit MAC tag. Accordingly, Zeidler describes to someone of ordinary skill in the art an *authentication tag formed by a truncation of the last ciphetext block* of standard CBC encryption (FIG. 13, element 184). There is no step of "after said applying step, combining said plurality of enciphered blocks to create an authentication tag." This step requires the "enciphered blocks" to already be in existence and then to combine them. It is not met by combining the result of a first cycle block with a next block of data prior to application to a next cycle block.

Additionally, Kanda is deficient in that it does not disclose performing a randomization function on each different data block to obtain input blocks, which are then applied to a pseudo-random function. Rather, Kanda discloses applying plaintext directly to

the cryptographic device. See Fig. 1 and column 9, lines 21-23. No reference to randomizing the data blocks is seen in Zeidler. Thus, the reference combination is also deficient in that the limitation "for each of said data blocks, performing a randomization function over said data block to create an input block of the same size as that of said data block" is missing.

Thus, the reference combination, even if it could be made (which it cannot), is deficient.

Finally, one of ordinary skill in the art could not combine the teachings of Zeidler in Kanda. Kanda's objective is to "permit fast encryption processing without involving a substantial increase in the number of rounds (col. 6, lines 13-19)." Any modification of Kanda with the standard block function used in Zeidler that increases the number of rounds would nullify Kanda for its intended purpose and would be meaningless to anyone regardless of how skilled in the art. References must be taken as a whole for what they teach to one of ordinary skill and modifications cannot be made that would nullify the intended purpose of the references.

The dependent claims are allowable for the reasons stated above. Additionally, each independent claim is allowable in view of the additional limitations set forth therein. Only selected dependent claims will be discussed in this response for purposes of brevity.

Regarding claims 34-35, Zeidler makes it clear (e.g., col. 15, lines 54-67 and in FIG. 13) that it is using the standard CBC-MAC, which is a *sequential* process as opposed to a *concurrent* process as set forth in these claims. The processing performed in Zeidler is *sequential* (Zeidler, col. 2, lines 6-13) and *not concurrent*, as required by claims 34 and 35.

Regarding claims 2, 62 and 72, the pseudo-random function is required to be a standard block cipher and this is not disclosed by Kanda. In the section of Kanda cited as support for this limitation (col. 1, lines 18-30), Kanda describes the prior art of his invention (e.g., the Data Encryption Standard, DES) and *does not disclose a pseudo-random function that is a standard block cipher*. Instead, Kanda discloses a pseudo-random function that is *unlike the standard DES*, which he says could be easily broken ("Biham et al say that DES could be broken by this cryptoanalysis if 2.sup.47 sets of plaintext-ciphertext pairs are

available" col. 3., lines 54-56, and "[s]ince DES has the defect that the main key can easily be derived from the subkey" col. 4, line 67 – col 5, line 1). Thus, Kanda does not disclose this limitation.

Regarding claims 4-5, the limitation is added of creating a random vector block of l bits. Fig. 4, element 302 of Kanda is cited as disclosing this element. However, in Fig. 4, element 302, Kanda performs a key-dependent initial transformation on the input. This is done within the block cipher (which is the subject of Kanda's invention) and hence *after* the data block is input to the block cipher (viz., Fig. 4, elements 301 and 302). In contrast, Applicant's Claim 4 requires "creating a random vector block of ℓ bits in length and then applying a pseudo-random function to the random vector block" and claim 5 requires "performing the randomization function over the random vector block to obtain a randomized random vector block, and then applying the pseudo-random function to the randomized random vector block." This language requires performing the randomization function over the random vector block in claim 5 *before* the data blocks and random vector block are input to the block cipher. This claim limitation is important because it allows use of a pseudo-random function that is a standard block cipher whereas Kanda as modified by Zeidler cannot. Also, Kanda as modified by Zeidler does not create a random vector independent of the data or input blocks being processed.

Regarding claims 26, 30, 45, 83, 85, 88 and 91 that claim the combination operation using a bitwise exclusive-or operation, the reference Zeidler at Fig. 13, element 168 is cited. However, as noted previously, in Fig. 13, element 168 Zeidler discloses the use of an exclusive-or operation within the standard CBC encryption mode that combines a *plaintext input* block with a previously obtained *ciphertext output* block to create the input block for the next block cipher (Zeidler, col. 15, lines 56-63). The exclusive-or operation used by Zeidler (element 168) is in no way related to the authentication tag of Zeidler, which is simply the truncation to 24 bits of the last ciphertext block and is not combined with anything (Zeidler, col 16, lines 1-3). In contrast, in the above listed claims, the exclusive-or operation is used to combine existing ciphertext output blocks to create the authentication tag, so that the teaching of Zeidler does not meet this element.

Claims 27-28 and 50-51 require the combination operation that follows the applying the pseudo-random function operation to be a modulo operation. Although Kanda and Zeidler do not disclose addition modulo or subtraction modulo, the reference Jones is cited to remedy this deficiency in the combination. However, Jones, uses modular addition and subtraction *inside encryption operations* for secret and public key encryption algorithms. See Fig. 15D of Jones and its description at columns 7-8. But the referenced claims use modular addition and subtraction *outside encryption operations* and *separately* from them. Specifically, the combining step is occurring after the pseudo-random function has been performed and functions to operate on the results ("the enciphered blocks") of applying the pseudo-random function on each of the input blocks. Further unlike Jones, these claims use modular addition and subtraction for combining ciphertext blocks to obtain an authentication tag. This use of modular addition or subtraction is not disclosed by Jones, Kanda and Zeidler. Hence, it would be impossible to anyone, no matter how skilled in the art, to use "the system of Kanda and Zeidler as Jones teaches so as to compute the authentication tag algorithms" as asserted by the Office Action.

The examiner's indication of allowable subject matter is appreciated for claims 7-25, 29-33, 37-48 and 82-85.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of

papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date 10/13/05 By _____

FOLEY & LARDNER LLP
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5143
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

William T. Ellis
Attorney for Applicant
Registration No. 26,874